WHAT IS CLAIMED IS:

1. In a public key encryption system, a method for selecting a current secret key to be used to encrypt a message, the method comprising:

determining whether a new secret key is required;

if a new secret key is required:

generating the new secret key;

generating a new encrypted secret key by encrypting the new secret key using a public key associated with a recipient of the message;

storing in a local data store the new secret key as a reusable secret key, the new encrypted secret key as a corresponding reusable encrypted secret key, and counter data associated with the reusable secret key; and

selecting as the current secret key the new secret key; and

if a new secret key is not required:

retrieving from the local data store a reusable secret key and the corresponding reusable encrypted secret key;

updating the counter data associated with the reusable secret key in the local data store; and

selecting as the current secret key the reusable secret key.

2. The method of claim 1, further comprising storing in the local data store state information associated with a cryptographic algorithm in which the reusable secret key is applied.

3. The method of claim 1, wherein determining whether a new secret key is required comprises:

determining whether a previous message has been sent to the recipient;

if a previous message has not been sent to the recipient, determining that a new secret key is required; and

if a previous message has been sent to the recipient:

retrieving the counter data from the local data store; and

comparing the counter data to a reuse criterion;

if the counter data satisfies the reuse criterion, determining that a new secret key is not required; and

if the counter data fails to satisfy the reuse criterion, determining that a new secret key is required.

4. The method of claim 3, wherein the reuse criterion comprises a maximum number of messages and the counter data comprises a cumulative number of messages previously sent using the reusable secret key.

5. The method of claim 3, wherein the reuse criterion comprises a maximum number of bytes of message data and the counter data comprises a cumulative number of bytes of message data previously sent using the reusable secret key.

6. The method of claim 3, wherein the reuse criterion comprises a maximum amount of elapsed time and the counter data comprises an amount of elapsed time since the reusable secret key was generated.

7. The method of claim 1, further comprising:

encrypting the message using the current secret key; and

sending the encrypted message and the encrypted secret key.

8. In a public key enveloping system, a method of decrypting a received message comprising:

extracting an encrypted secret key from the received message;

determining whether the encrypted secret key was previously decrypted;

if the encrypted secret key was not previously decrypted:

decrypting the encrypted secret key; and

storing the encrypted secret key and the decrypted secret key in a local data store;

if the encrypted secret key was previously decrypted, retrieving the decrypted secret key from the local data store; and

decrypting the message using the decrypted secret key.

9. The method of claim 8, wherein determining whether the encrypted secret key was previously decrypted comprises:

searching for the encrypted secret key in the local data store;

if the encrypted secret key is found in the local data store, determining that the encrypted secret key was previously decrypted; and

if the encrypted secret key is not found in the local data store, determining that the encrypted secret key was not previously decrypted.